# DataHarbor™ Network Backup Appliance User Manual

- **Ease of Use** – Fast setup, easy rotation, fast recovery. When it's time to swap drives, simply pull the drive and insert another.
- **Scheduled Backup** – Create the backup schedule that works for you and your networked PCs with the easy-to-use Microsoft Storage Server Essentials software.
- **Remote Administration** – Administrators can update or change the DataHarbor configuration over the network. Email and/or text message notifications.
- **Whole Disk Encryption** – CRU's transparent hardware encryption secures the entire disk, which is better than software-based encryption since hackers can't even find the file allocation table. Combined with 256-bit AES encrpytion, this means your data is safe from attack.

## Table of Contents


| | |
|---|---|
| **1. Pre-Installation Steps** | |
| 1.1 Accessories | 2 |
| 1.2 Identifying Parts of Your DataHarbor | 2 |
| 1.3 Warnings and Notices | 3 |
| 1.4 Additional Online Help | 3 |
| **2. Installation Steps** | |
| 2.1 Mounting Options | 3 |
| 2.2 Windows Storage Server 2008 R2 Essentials Setup Procedure | 4 |
| 2.3 Connecting the DataHarbor to a Network | 4 |
| 2.4 Joining a Domain | 5 |
| 2.5 Joining a HomeGroup | 5 |
| 2.6 Installing Connector Software on Client Computers | 5 |
| 2.6.1 Install Dashboard and Launchpad on Windows | 5 |
| 2.6.2 Install Launchpad on Mac | 6 |
| **3. Server Management** | |
| 3.1 User Account Management | 7 |
| 3.2 Server Folder and Hard Drive Management | 7 |
| 3.3 Manage Backups | 8 |
| 3.3.1 Configuring Automatic Backups for Mac OS | 8 |
| 3.4 Set Up Remote Access | 10 |
| 3.5 Manage Alerts | 10 |
| 3.6 Manage Add-Ins | 11 |
| 3.7 Shut Down or Restart the DataHarbor | 11 |
| 3.8 Other Server Settings | 11 |
| **4. Restore Lost Files or Folders** | |
| 4.1 Create a Client Recovery Thumb Drive | 11 |
| 4.2 Full Windows Client System Restore | 12 |
| 4.3 Restore Files From Windows Client Computers | 12 |
| 4.4 Restore Files From Mac Client Computers | 12 |
| **5. Restore a DataHarbor Server** | |
| 5.1 Restore From A Failed Primary Hard Drive | 12 |
| 5.2 Rebuild a Degraded RAID | 13 |
| 5.3 Restore to a New DataHarbor with Identical Hardware | 13 |
| 5.4 Restore to a New DataHarbor From an Encrypted Backup Drive | 13 |
| 5.5 Migrate Data to a Newer Version of DataHarbor | 14 |
| **6. Buzzer and Temperature Configuration** | 15 |
| **7. Best Practices for a Proper Backup Strategy** | 16 |
| **8. Encryption** | 16 |
| **9. Technical Specifications** | 17 |


# 1. Pre-Installation Steps

## 1.1 Check the Accessories with Your DataHarbor

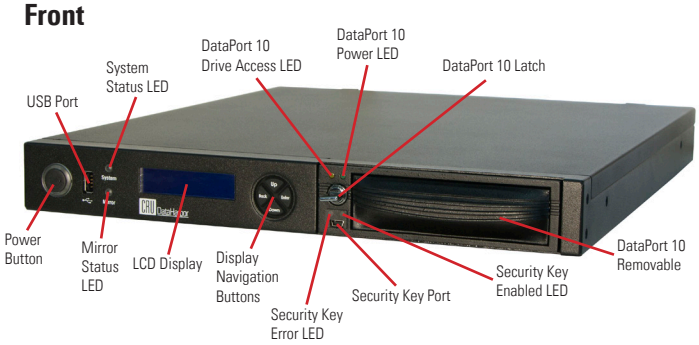
Please contact CRU-DataPort if any items are missing or damaged. The box should contain the following items:

| Accessories | Quantity |
|---|---|
| DataHarbor | 1 |
| Power Cord | 1 |
| Ethernet Cable | 1 |
| Hard Drive Carrying Case | 2 |
| Stand Kit<br>- Thumb Screw<br>- Flat Stand Bracket<br>- Rubber Foot | 1<br>2<br>2<br>4 |
| Rack Mount Kit<br>- Ear Mounting Bracket<br>- Large S-Bracket<br>- Small S-Bracket<br>- Packet of Rack Mounting Screws | 1<br>2<br>2<br>2<br>1 |
| Thumb Drive for Client Recovery | 1 |
| Security Key | 3 |
| Lanyard for Security Key | 3 |
| Security Key ID Tag | 3 |
| Security Key Label | 6 |

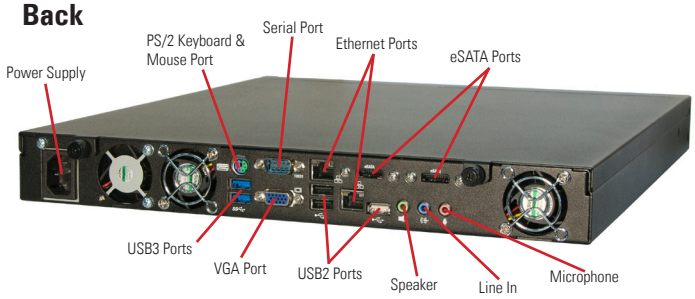
## 1.2 Identifying Parts of Your DataHarbor

Take a moment to familiarize yourself with the parts of DataHarbor. This will help you to better understand the remaining instructions.

### Front




### Back



## 1.3 Warnings and Notices

*Please read the following before beginning installation.*

### General Care

- The main circuit board of the HDD carrier is susceptible to static electricity. Proper grounding is strongly recommended to prevent electrical damage to the enclosure or other connected devices, including the computer host. Avoid all dramatic movement, tapping on the unit, and vibration.
- Avoid placing the HDD carrier close to magnetic devices, high voltage devices, or near a heat source. This includes any place where the product will be subject to direct sunlight. Do NOT allow water to make contact with the carrier or receiving frame.
- Before starting any type of hardware installation, please ensure that all power switches have been turned off and all power cords have been disconnected to prevent personal injury and damage to the hardware.
- To avoid overheating, the DataHarbor should be operated in a well-ventilated area.

### RAID Backup

- Use only hard drives that are in perfect condition. Avoid using drives that have ever developed bad sectors during previous usage. This could lead to possible device failure or loss of data.
- The DataHarbor supports SATA hard drives of various specifications and different capacities. However, we recommend using drives of the same capacity, cache, and transfer speed for optimal performance. If drives of different capacities are used in a RAID, the capacity of the smallest drive will determine how much of each drive is used. The additional capacity on the larger drives will not be used by the RAID.

### Encryption

- Though the Security Key port is mechanically identical to the standard Mini-USB port, inserting Security Keys into any other Mini-USB port may damage the keys and render them useless. Please only use Security Keys in CRU-DataPort products.

  Likewise, inserting a Mini-USB cable or other device into the DataHarbor Security Key port on the carrier may cause internal damage and potentially lead to loss of data.

### Case Maintenance

The DataHarbor case cover is secured by two thumb screws as well as one additional Phillips-head safety screw in order to comply with IEC60950-1 safety regulations. Do not remove the safety screw unless you are a certified IT professional performing maintenance on the DataHarbor.

### Key Management

The DataHarbor encrypts your backup drives using a special Security Key inside of the DataHarbor. Two additional Security Keys have been included in your accessories box. These keys can be used to recover your data from your backup drives should your DataHarbor be stolen or suffer catastrophic damage. Always store these keys offsite and away from your backups so that in the event of a catastrophe (fire, flood, etc.) your backup data will remain retrievable. **There is no "back door" to access the data; lost keys make data recovery virtually impossible.**

## 1.4 Additional Online Help

Windows Storage Server 2008 R2 Essentials contains secondary features not necessary for normal operation of your DataHarbor. Additional online help for these and the primary features discussed herein can be found on Microsoft Technet: http://technet.microsoft.com/en-us/library/ff953176.

# 2. Installation Steps

## 2.1 Mounting Options

### 2.1.1 Horizontal Orientation

Place the rubber feet from the stand kit on each of the four bottom corners of the DataHarbor and set it in a clear area.

### 2.1.2 Vertical Orientation

Use the thumb screws from the stand kit to secure the flat stand brackets to the right side of the DataHarbor case. The metal tabs on the brackets should face away from the cover to allow access to the inside of the DataHarbor while it is standing in vertical position. Once the brackets are installed, place two rubber feet on the bottom of each bracket.

### 2.1.3 Front Rack Mount

The DataHarbor can be mounted into a four-post rack using just the ear mount brackets from the rack mount kit, providing your four-post rack is strong enough to support the weight. Attach the ear mount brackets to the front of each side of the DataHarbor. Rotate the ear mount brackets so that the short ends face outward from the sides of the DataHarbor and screw them in using the provided short screws.

### 2.1.4 Slide Rack Mount

To use the DataHarbor with CRU-DataPort's slide rail kit, first attach the ear mount brackets to the front of each side of the unit. Rotate the ear mount brackets so that the short ends face outward from the sides of the DataHarbor and screw them in using the provided short screws. Leave the middle screw hole open.

Next, use the provided long screws to attach the large S-brackets to middle of the ear mount brackets. Ensure the threaded screw hole is attached to the DataHarbor. Finally, use the provided short screws to attach the small S-brackets to the dual holes on the rearward sides of the DataHarbor. Ensure the threaded screw holes are attached to the DataHarbor.

Your DataHarbor is now ready to be used with the CRU-DataPort slide rail kit.

#### 2.1.5 Rack Mounting Warnings

**Elevated Operating Ambient Temperature:** The operating ambient temperature of the rack environment may be greater than the room ambient temperature if the enclosure is installed in a closed or multi-unit rack assembly. Install the equipment in an environment compatible with the maximum ambient temperature of 40° C.

**Reduced Air Flow:** Do not block or inhibit the air flow required for safe operation of the enclosure.

**Mechanical Loading:** Use care when mounting the rack in order to prevent injury.

**Circuit Overloading:** Do not overload the circuits. Refer to the name plate ratings on the equipment.

**Reliable Grounding:** Maintain reliable grounding of rack-mounted equipment by using indirect connections to the branch circuit (i.e. UPS battery backups, power strips).

**Removing the Cover:** Turn off and unplug the enclosure before removing the cover.

### 2.2 Windows Storage Server 2008 R2 Essentials Setup Procedure

You will need a keyboard, mouse and monitor. Ensure that the secondary hard drive is installed inside of the DataPort 10 and is locked into place, then follow these instructions:

a. Before turning the DataHarbor on, ensure that the removable drive that came packaged with the DataHarbor is inserted into the empty bay. Then lock it into place by turning the latch so that it is horizontal.

b. Boot up the DataHarbor. The LCD readout should show **MIRROR STATUS: NORMAL**. If you do not get this message, refer to the note just below.

**NOTE:** If the DataHarbor alarms, do not proceed with setup. Mute the alarm by pressing the **Enter** button on the front of the DataHarbor. You can then pull out the removable drive and continue with setup, opting to rebuild the RAID mirror later. Or you can rebuild the mirror first, referring to Section 5.2 for instructions. A mirror rebuild will take several hours to complete. **Do not attempt to complete the setup process while a mirror rebuild is underway.**

c. After a few moments, the setup process for Windows Storage Server 2008 R2 Essentials will begin. Follow the prompts and provide the needed information for each.

d. The setup program will then begin finishing the installation process, which can take up to an hour to complete. The system may reboot several times. Once the setup program displays "Your server is now ready to use", the setup has completed and you can click the Close button to log in to the server desktop.

### 2.3 Connecting the DataHarbor to a Network

Insert an Ethernet cable from your network into the Ethernet port located above the USB 2.0 ports. This is the port for Local Area Connection in the server's Network Connections list.

#### 2.3.1. DHCP

On DHCP networks, a new IP address is dynamically assigned to the DataHarbor as soon as the network detects it. No configuration is required. You can determine the address by performing the following actions:

a. Click on the Start Menu → Run, type in cmd, and click OK.

b. On the Command Prompt window that opens, type in ipconfig. The IP address is listed under the entry for "IPv4 Address".

#### 2.3.2 Static Network

a. Click on the **Start Menu → Control Panel**.

b. In the Control Panel, under Network and Internet, select **View network status and tasks**.

c. Click on **Change adapter settings** in the sidebar.

d. Right click on the **Local Area Connection** and select **Properties**.

e. In the Local Area Connection Properties window that pops up, select **Internet Protocol Version 4 (TCP/IPv4)** from the list and click on the **Properties** button.

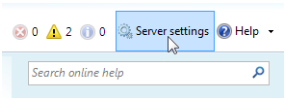
f. Select the **Use the following IP address** radio button and enter in the **IP address**, **Subnet mask**, and **Default gateway** addresses appropriate to your server configuration.

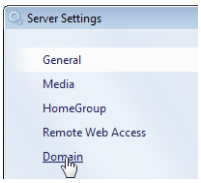
g. Select the **Use the following DNS server addresses** radio button and enter in the **Preferred DNS server** and **Alternate DNS server** addresses.

h. Click **OK** and close the Network Connections window.

## 2.4 Joining a Domain

a. Open the Dashboard program and select **Server Settings** from the toolbar on the right side of the window.




b. Select **Domain** from the list on the left.

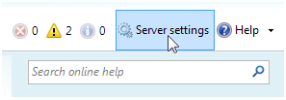
c. Type in the name of the domain name in the text field and then click the **Join domain** button.

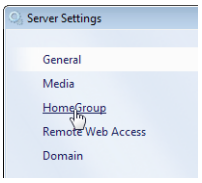
d. Restart the server for changes to take effect.

Joining a domain requires managing users differently than the instructions described in this document. For instructions on how to manage domain users in Windows Storage Server 2008 R2 Essentials, refer to the Microsoft Technet Website: http://technet.microsoft.com/en-us/library/manage-domain-users-3

## 2.5 Joining a HomeGroup

You can join the server to an already existing HomeGroup by following these instructions:




a. Open the Dashboard program and select **Server Settings** from the toolbar on the right side of the window.

b. Select **HomeGroup** from the list on the left.

c. Click on the **Join now…** button.

d. Type in the HomeGroup password and click the **Join now** button.

## 2.6 Installing Connector Software on Client Computers

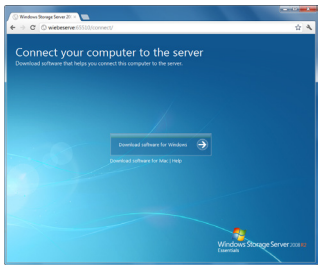
### Dashboard vs. Launchpad

Dashboard is the server administration program that allows system administrators to fully manage the server from a client PC or from the server itself. Dashboard is only available on Windows PCs. In order to maintain a secure server environment, it is recommended that system administrators manage the server via a client PC instead of logging directly into the server itself. The Dashboard requires the server's local administrator account password in order to log in.

Launchpad is a server access program that allows users to manage their client PC's backup settings, use Remote Web Access, access shared folders on the server, and launch the Dashboard program. Launchpad is available on both Windows PCs and Macs. In order to log in, a user account must be created on the server from the Dashboard, which allows system administrators to set basic accessibility permissions for different users (see Section 3.1). The user would then log in utilizing the account's username and password.

### 2.6.1 Install Dashboard and Launchpad on Windows

a. On the client computer, open a web browser and type the following into the URL field and press **Enter**: http://<ServerName>/connect. The <ServerName> is the name you assigned your server during the setup process.

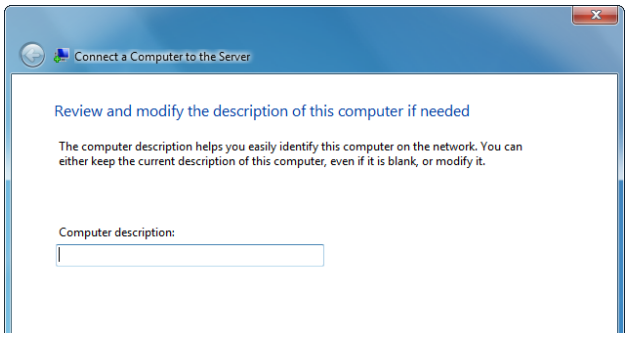



b. The browser will open a page with a button on it asking you to download software. Click on the button, download and open the software setup program.

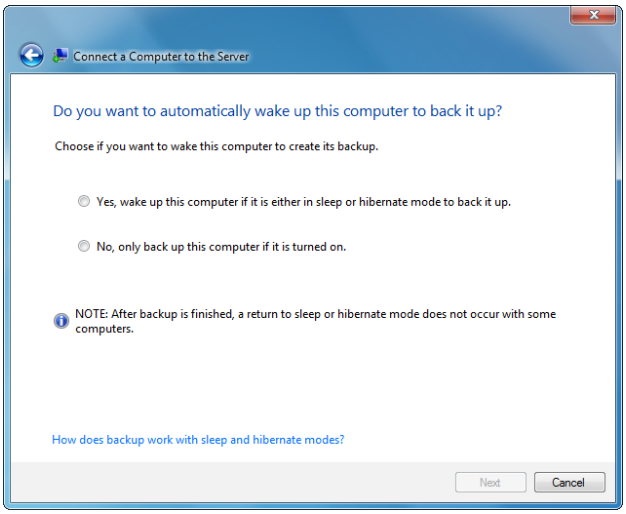
c. Click the **Next** button until the program begins verifying and installing necessary components. When it is done, it will ask you for the server password. Type in the password and click **Next**.

Connect a Computer to the Server
Log on to your Windows Storage Server 2008 R2
Enter the Windows Storage Server 2008 R2 password:

d. Add a description for the client computer and click **Next**.

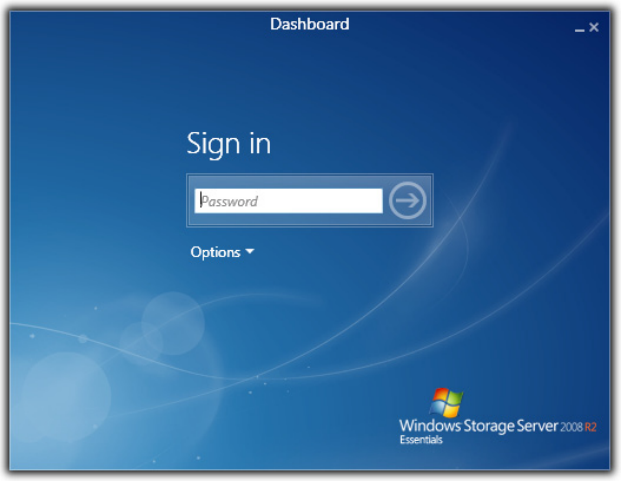

Connect a Computer to the Server
Review and modify the description of this computer if needed
The computer description helps you easily identify this computer on the network. You can either keep the current description of this computer, even if it is blank, or modify it.
Computer description:

e. Choose whether or not you would like to wake the computer when the server attempts to back it up and then click **Next**.


Connect a Computer to the Server
Do you want to automatically wake up this computer to back it up?
Choose if you want to wake this computer to create its backup.
Yes, wake up this computer if it is either in sleep or hibernate mode to back it up.
No, only back up this computer if it is turned on.
NOTE: After backup is finished, a return to sleep or hibernate mode does not occur with some computers.
How does backup work with sleep and hibernate modes?
Next
Cancel

f. Choose whether you would like to participate in the Windows Customer Experience Improvement Program and click **Next**.

g. The setup program will now configure your computer and install the Dashboard software. When it is finished, you can optionally choose to launch Dashboard. If you do so, it will ask you for the server's local administrator account password. Type in the password and click the **Right arrow** to log into the Dashboard.

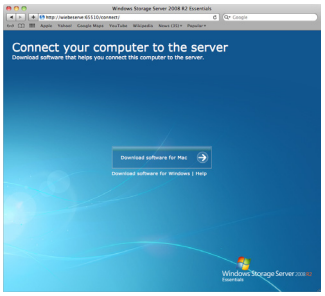



To access the Dashboard or Launchpad, open the **Start Menu** and navigate to **All Programs → Windows Storage Server 2008 R2** and click on the appropriate list item.

### 2.6.2 Install Launchpad on Mac

Dashboard is not available on Mac OS. However, many of the most common tasks can still be accomplished from the Launchpad. Install Launchpad by following the instructions below.

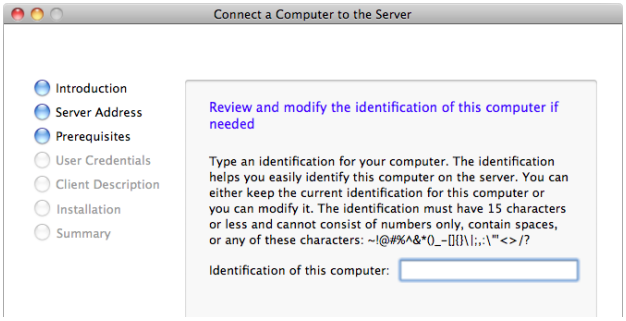
a. On the client computer, open a web browser and type the following into the URL field and press **Enter**: http://<ServerName>/connect. The <ServerName> is the name you assigned your server during the setup process.




b. The browser will open a page with a button on it asking you to download software. Click on the button, download and open the software setup program.

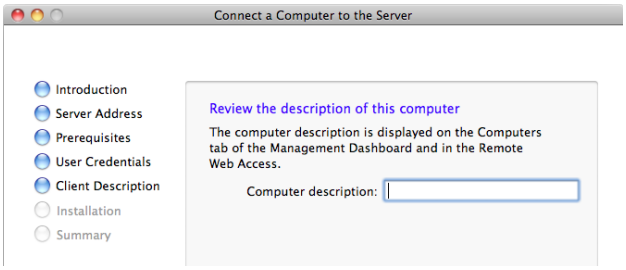
c. Click the **Continue** button and enter the server's address in the field. The address is the <ServerName> you entered in Step A. Click **Continue**.

d. The program will verify that the Mac meets the server's requirements. When it does, name your computer and click **Continue**. This name will appear as the Computer's name in the Computers and Backup icon on the Dashboard.

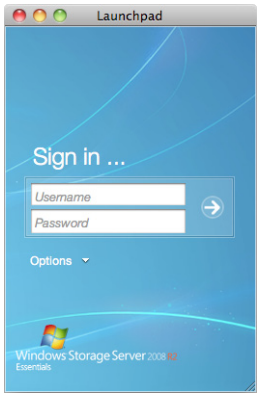

Connect a Computer to the Server
Introduction
Server Address
Prerequisites
User Credentials
Client Description
Installation
Summary
Review and modify the identification of this computer if needed
Type an identification for your computer. The identification helps you easily identify this computer on the server. You can either keep the current identification for this computer or you can modify it. The identification must have 15 characters or less and cannot consist of numbers only, contain spaces, or any of these characters: ~!@#%^&*()_-{}[]\|;:\'"<>,/?
Identification of this computer:

e. Enter the server's password and click **Continue**.

f. Add a description for the client computer and click **Continue**.



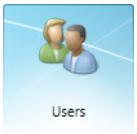

g. The program will now show that the computer is now connected to the server. You can optionally choose to open Launchpad automatically at startup before clicking on the **Close** button. If you do so, Launchpad will open and will ask you for a username and password. Usernames must be assigned by the server Administrator from the Dashboard (see Section 3.1). Type in the username and password and click the **Right arrow** to log into the Dashboard.




To access Launchpad, open a **Finder** window, click on **Applications** in the sidebar, and then scroll down to double-click on **Windows Server Launchpad**.

# 3 Server Management

## 3.1 User Account Management




User accounts are necessary to allow users limited access to the server via the Launchpad. On the Dashboard, click the **Users** icon. The following table describes the various server folder tasks that are available in the task pane to the right. Some of the tasks are account specific, and are only visible when you select an account in the list.

| Task Name | Description |
|---|---|
| View the account properties | Displays the properties of the selected user account.<br><br>**General Tab**<br>• Change the user account owner's first and last names<br>• Change the account password<br>• Activate or deactivate the account<br>• Determine whether users logged in under the account can view network health alerts<br><br>**Shared Folders Tab**<br>• Change the account's access permissions to the server's folders<br><br>**Remote Web Access Tab**<br>• Select which server assets are accessible to this account via Remote Web Access |
| Deactivate the user account/ Activate the user account | • Deactivating a user account closes down, but does not delete the account<br>• Activating a user account reactivates a previously deactivated user account |
| Remove the user account | Deletes the user account. |
| Change the user account password | Allows you to change the user account's password. |
| Add a user account | Allows you to create a user account and assign access permissions to the server. |
| Set the password policy | Lets you determine the complexity of the passwords used for each user account.<br><br>**Weak**: Any non-blank password is accepted<br>**Medium**: Passwords must contain at least 5 characters<br>**Best**: Passwords must contain at least 5 characters and must include letters, numbers, and symbols<br>**Strong**: Passwords must contain at least 7 characters and must include letters, numbers, and symbols |

## 3.2 Server Folder and Hard Drive Management

### 3.2.1 Server Folders

On the Dashboard, click the **Server Folders and Hard Drives** icon and click on the **Server Folders** tab. The following table describes the various server folder tasks that are available in the task pane to the right. Some of the tasks are folder specific, and are only visible when you select a folder in the list.

| Task Name | Description |
|---|---|
| Open the folder | Displays the contents of the folder. |
| Delete the folder | Allows you to delete the folder. This task is not available for the default folders created by Windows Storage Server 2008 R2 Essentials. |
| View the folder properties | Displays the properties of the selected folder.<br><br>**General Tab**<br>• Rename user-created folders<br>• Change the description of the folder<br>• Open the folder in Windows Explorer<br><br>**Sharing Tab**<br>• Modify user account access permissions for the folder |
| Move the folder | Opens the Move a Folder Wizard that will allow you to move the folder to a new location. |
| Stop sharing the folder | Prevents users from accessing the folder. |
| Add a folder | Opens the Add a Folder Wizard which allows you to create a folder and assign permissions. |
| Understanding Server Folders | Opens a Microsoft Online Help web page that further explains the usage of server folders for centralized storage. |

### 3.2.2 Hard Drives

On the Dashboard, click the **Server Folders and Hard Drives** icon and click on the **Hard Drives** tab. The following table describes the various hard drive tasks that are available in the task pane to the right. Some of the tasks are hard drive specific, and are only visible when you select a drive in the list.

| Task Name | Description |
|---|---|
| View the hard drive properties | Displays the properties of the selected hard drive.<br><br>**General Tab**<br>• Allows you to rename the hard drive<br>• Access the Disk Cleanup wizard<br>• Check and repair problems with the hard drive<br><br>**Shadow Copies Tab**<br>• Enable or disable shadow copies, which allow users to access files and folders as they were at a previous point in time. |
| How do I increase storage on the server? | Opens a Microsoft Online Help web page for adding additional storage. CRU-DataPort does **not** recommend following these instructions for adding storage, as it will require disabling the DataHarbor's RAID mirror of the server. |

## 3.3 Manage Backups

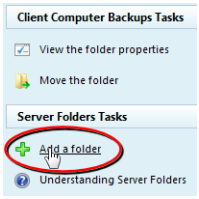
Backup is automatically set up the first time that the connector software is installed on a client PC and the PC is joined to the server. No additional configuration is necessary.

Macs will have to be configured independently. See Section 3.3.1 for detailed instructions.

On the dashboard, click on the **Computers and Backup** icon. The following table describes the various backup tasks that are available in the task pane to the right. Some of the tasks are computer or server specific, and are only visible when you select a computer or the server in the list.

| Task Name | Description |
|---|---|
| View the computer/ server properties | Allows you to view basic information about the computer (name, description, OS) and the computer's or server's backup history. |
| Start/Stop a backup for the computer | Begins or stops a manual backup of the server. |
| Restore files or folders for the computer | Allows the user to choose a specific backup to restore to the computer. |
| Customize Backup for the computer | Allows you to add or remove backup items or disable backup for the client computer. |
| Customize Backup for the server | On first use, this opens the Set Up Server Backup Wizard, which allows you to set up a backup for the server to an external or network drive. For most configurations, it is not necessary to set a server backup since the server is already backed up to the removable hard drive inside the DataHarbor. |
| Remove the computer | Removes the client computer from the server. The client computer will no longer be able to access server resources and the server will be unable to manage the client computer. |
| View alerts for the server | Opens the Alert Viewer. |
| Additional client computer backup tasks | Allows you to modify the server's backup tasks.<br><br>**Settings Tab**<br>• **Client computer backup schedule**: Set the start and end time during which client computers will be backed up.<br>• **Client computer backup retention policy**: Set how long daily, weekly, and monthly backups are retained before they are deleted from the server.<br><br>**Tools Tab**<br>• **Repair backups**: Attempts to repair client computer backups if they become unstable.<br>• **Computer recovery**: Allows you to create a key to restore a client computer from an existing backup. This option requires the use of a USB flash drive. |
| Change the server password | Allows you to change the server's password. |
| How do I connect computers to the server? | Opens a Microsoft Online Help web page for connecting client computers to the server. |

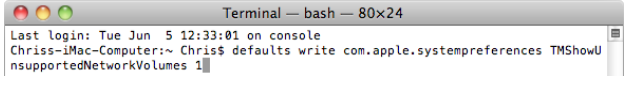
### 3.3.1 Configuring Automatic Backups for Mac OS




a. Open the Dashboard from a PC and create a new server folder for Mac backups. Go to the **Server Folders and Hard Drives** icon, make sure the **Server Folders** tab is selected, and then click on **Add a folder** in the tasks pane. Name your folder and then click **Next**. Click on the **Specific people** icon, and then make sure the access level for the user account you are assigning to the Mac computer is set to full Read/Write access. Click **Add a folder** to create the folder.

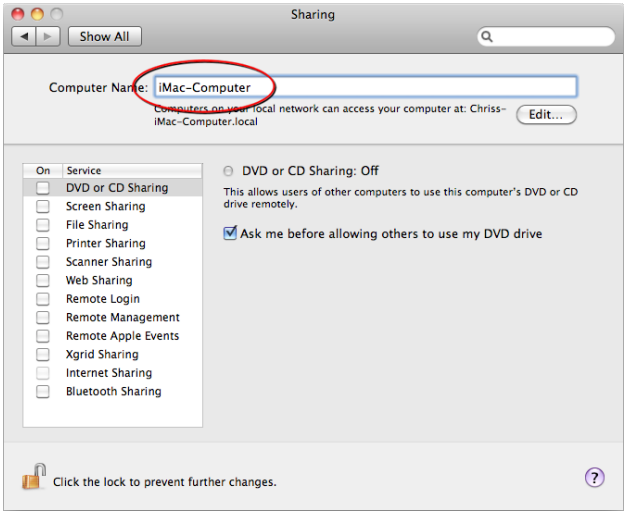
b. Enable unsupported network volumes so they can be detected by Time Machine. On the Mac Finder, select the **Go** menu and click on **Utilities**. Open **Terminal** and type in the following:

*defaults write com.apple.systempreferences TMShowUnsupportedNetworkVolumes 1*


Terminal — bash — 80×24
Last login: Tue Jun 5 12:33:01 on console
Chriss-iMac-Computer:~ Chris$ defaults write com.apple.systempreferences TMShowU
nsupportedNetworkVolumes 1

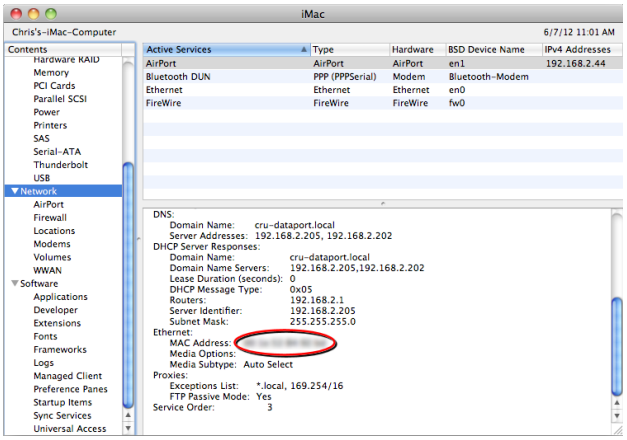
Hit **Enter**. If you typed it in right, no extra text aside from another prompt should print in the window. This will enable Time Machine to view the Mac backups folder you just created on your DataHarbor, provided you do not reboot the machine before finishing this process. If you do, simply repeat this step to re-enable support for unsupported network volumes.

c. Obtain the Mac's computer name for use in Step E. Open the **Apple** menu and select **System Preferences…** Click on the **Sharing** icon. Your computer name is shown at the top of the window.



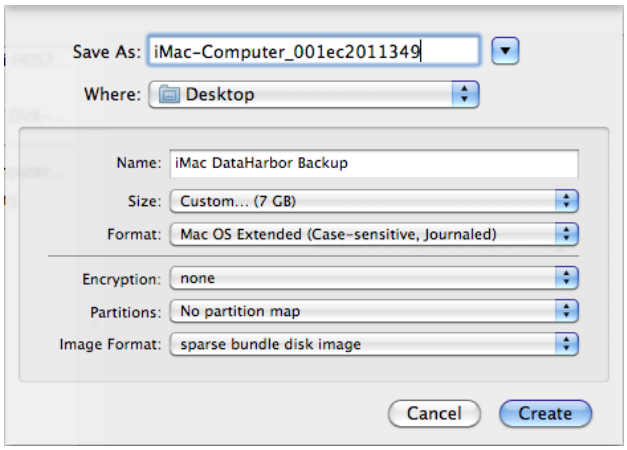

d. Obtain the Mac's Ethernet port MAC address for use in Step E. Open the **Apple** menu and select **About This Mac**. Click on the **More Info…** button. Click on **Network** and then choose **Ethernet** from the list of Active Services in the upper right-hand pane. Below, scroll down to where it says **MAC Address**. The series of 6 numbers separated by colons is your MAC Address.

Ensure that the MAC Address you select is the Mac's Ethernet port's. The Airport Mac Address, even if you are connected to the network via Airport, will not allow the backups to work.



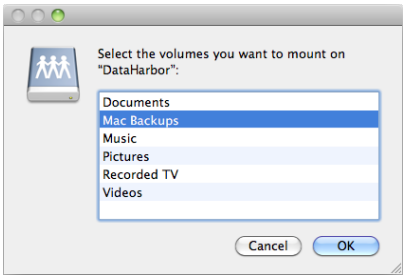

e. Create a sparse bundle disk image for Time Machine. On the Mac Finder, select the **Go** menu and click on **Utilities**. Open **Disk Utility** and select the **New Image**. Use the following settings:

**Save As**: <computer name>_<MAC address without colons>
**Where**: Desktop
**Name**: <The name can be anything you like>
**Size**: <Set the size according to how large you think your largest backup should be. A default Time Machine backup on a new Mac is usually around 6.5-7 GB.>
**Format**: Mac OS Extended (Case-sensitive, Journaled)
**Encryption**: none
**Partitions**: No partition map
**Image Format**: sparse bundle disk image



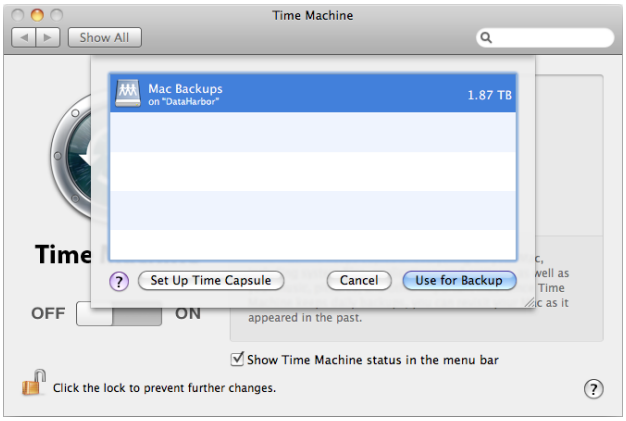

Click **Create**. A disk image will mount on the desktop along with the .sparsebundle file. Feel free to eject the disk image as it is not needed.

f. Copy the sparse bundle image to your Mac backups folder on the DataHarbor. On the Finder, select the **Go** menu and click on **Connect to Server…** Type in **smb://<servername>** where <servername> is the name of your server and click **Connect**. The Mac will connect to the DataHarbor and will prompt you to enter the DataHarbor user name and password assigned to the Mac. Do so and then click **OK**. You will now see a window asking you to select the volumes you want to mount. Select your **Mac Backups** folder and click **OK**. The folder will open in a new window. Drag the sparse bundle disk image file on your Desktop over to the window to copy it over.




g. Configure your Time Machine backup. Open **Time Machine Preferences** by opening the **Apple** menu and selecting **System**

**Preferences…** Click on the **Time Machine** icon. If this is your first time using Time Machine, click the **Select Backup Disk…** button. If you have a previous Time Machine setup, click the **Select Disk** button. Your Mac backups folder should appear in the list. Select it and click **Use for Backup**. The Mac will ask you to enter the DataHarbor user name and password assigned to the Mac. Enter the information and click **Connect**.

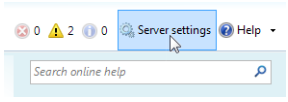


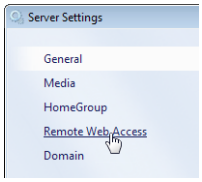

Your Mac backup is now configured! In about two minutes, the first backup will automatically start. While you will not be able to see the percentage completion in the Dashboard's Computers and Backup section like you can with PCs that are performing a client backup, you will be able to see the Backup status, and the server will notify you of any Alerts pertaining to the backup.

## 3.4 Set Up Remote Access

### 3.4.1 Turn on Remote Access

a. Open the Dashboard and select **Server Settings** from the toolbar.

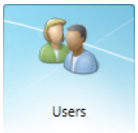


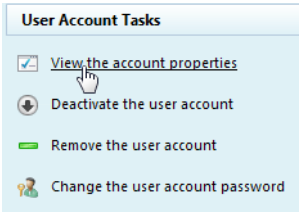

b. Click on **Remote Web Access** from the sidebar on the left.

c. Click the **Turn on** button and complete the wizard.

### 3.4.2 Manage Remote Web Access Permissions




a. Open the Dashboard and select the **Users** icon.


User Account Tasks
View the account properties
Deactivate the user account
Remove the user account
Change the user account password

b. Click on the user account you want to manage and then click **View the account properties** in the tasks pane on the right. The user account properties window will open.

c. In the **Properties** box, click the **Remote Web Access** tab.

d. Click the **Allow Remote Web Access and show selected links on Remote Access** radio button to enable Remote Access for this user account. Then select the assets the user account is allowed to access via Remote Web Access.

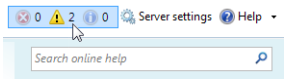
To turn off Remote Web Access for this account, select the **Do not allow Remote Web Access** radio button.

e. Click **OK**.

## 3.5 Manage Alerts

### 3.5.1 Organize Alerts

a. Open the Dashboard and select any of the **displayed alerts icons** on the toolbar, next to the **Server Settings** button. The Alert Viewer will open.




b. Click on the **Organize list** drop-down menu and select your desired option.

**Filter by computer** – Only the alerts for the selected computer will be displayed in the Alert Viewer.

**Filter by alert type** – Only the certain type of alert (Warning, Critical, or Informational) will be displayed in the Alert Viewer.

### 3.5.2 Delete Alerts

You can use the Alert Viewer on the Dashboard to delete an alert. If you delete an alert and the server detects the same problem, it will create a new alert.

a. Open the Dashboard and select any of the **displayed alerts icons** on the toolbar, next to the **Server Settings** button.

b. Right-click the alert that you want to delete and select **Delete the alert**.

c. The server will ask if you want to delete the alert. If so, click **Yes**.

### 3.5.3 Ignore Alerts

a. Open the Dashboard and select any of the **displayed alerts icons** on the toolbar, next to the **Server Settings** button.

b. Select the alert you want to ignore, and then select **Ignore the alert** from the Tasks section. This will disable and ignore the alert.

### 3.5.4 Enable Alerts

a. Open the Dashboard and select any of the **displayed alerts icons** on the toolbar, next to the **Server Settings** button.

b. Select the alert you want to enable, and then select **Enable the alert** from the Tasks section. This will enable the alert.

#### 3.5.5 Set up E-mail Alert Notifications

a. Open the Dashboard and select any of the **displayed alerts icons** on the toolbar, next to the **Server Settings** button.

b. At the bottom of the Alert Viewer, select **Set up email notification for alerts**.

c. Click on the **Enable** button.

d. Type in the SMTP server settings for your mail server and the e-mail address from which the alerts will be sent, then click **OK**.

e. Type in the e-mail recipients, separating each with a semicolon, and click the **Apply and send email** button to test that all the information has been set correctly.

f. If successful, click **OK** to to close the wizard and click the **Close** button to close the Alert Viewer. If unsuccessful, click **Change SMTP settings** to correct the server information.

### 3.6 Manage Add-Ins

You can perform certain administrative tasks by using the **Add-Ins** section of the Dashboard. On the dashboard, click on the Add-ins icon. The following table describes the various backup tasks that are available in the task pane to the right. Some of the tasks are Add-in specific, and are only visible when you select an Add-in in the list.

| Task Name | Description |
|---|---|
| Remove the add-in | Allows you to remove the add-in from the server and from all the computers on the network. |
| Install the add-in on computers | Allows you to schedule the installation of the add-in on all other computers in the network. |
| Get help with the add-in | Opens a web page where you can find help for using the Add-In. |
| Update the add-in | Download and install updates for add-ins already installed on the DataHarbor and network computers. |
| Renew the add-in subscription | Opens a web page where you can renew your add-in subscription. |
| How do I install or remove add-ins? | Opens a Microsoft Online Help web page for installing and removing add-ins. |
| Search for Add-ins at Microsoft Pinpoint | Opens the Microsoft Pinpoint website where you can search for, download, and install new add-ins. |

#### 3.6.1 Downloading and Installing an Add-In

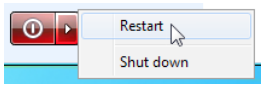
a. Open the Dashboard and click on the Add-ins icon. Click on the Search for Add-ins at Microsoft Pinpoint button in the task pane on the right. It will open a web page.

b. Search for your add-in from the site and download it.

c. Open the .wssx file. You will be prompted to enter the DataHarbor's administrator account password. Do so and then follow the setup instructions.

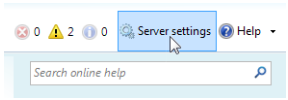
d. When the add-in is completely installed, it will show up in the listing on the Add-ins section of the Dashboard.

### 3.7 Shut Down and Restart the DataHarbor




To shut down or restart the DataHarbor, log into the Dashboard and click on the **Server Settings** button. In the lower left corner of the Server Settings window, you'll see a red button. Click on the arrow portion of the button and select your desired option.

### 3.8 Other Server Settings



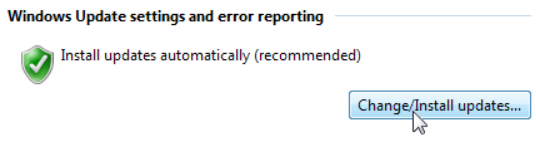

The following settings can be accessed by clicking on the **Server Settings** button on the Dashboard.

#### 3.7.1 Date, Time, and Region

Located in the General Tab, Date, Time, and Region allows you to change these settings.

#### 3.7.2 Windows Update

It is very important for the administrator to download and install new Windows updates each month. Updates are set by default to be downloaded and installed automatically. Sometimes this requires a server reboot, which ideally should be done before or after business hours. Change the Windows Update settings by clicking on the **Change/Install updates…** button in the General Tab.




#### 3.7.3 Media Server

The scope of this manual does not cover setting up a media server on the DataHarbor, nor is it supported by CRU-DataPort Technical Support. Should you wish to do so, follow the instructions at http://technet.microsoft.com/en-us/library/ff953176.aspx.

## 4 Restore Lost Files or Folders

### 4.1 Create a Windows Client Recovery Thumb Drive

a. Insert a blank thumb drive into the USB port on your DataHarbor server or client computer.

b. Open the Dashboard and click on the **Computers and Backup** icon.

c. Click on **Additional client computer backup tasks** in the tasks pane to the right.

d. Click on the **Tools** tab and select the **Create key…** button.

e. Follow the steps in the Create Computer Recovery Key Wizard.

### 4.2 Full Windows Client System Restore

a. Insert the client recovery thumb drive you created in Section 4.1 into a USB port on your client computer.

b. Boot into your computer's BIOS to ensure that the primary boot device is the client recovery thumb drive. See your motherboard's documentation for exact instructions.

c. Boot the computer and allow it to load the Windows Boot Manager from the thumb drive. Then select whether your computer is a 32-bit operating system or a 64-bit operating system.

d. Follow the steps in the Full System Restore Wizard.

### 4.3 Restore Files From Windows Client Computers

a. Open the Dashboard and click on the **Computers and Backup** icon.

b. Select the computer you want to restore and click **Restore files or folders for the computer** in the tasks pane to the right. The Restore Files or Folders wizard will open.

c. Select the backup that contains the files you want to restore and click **Next**. The wizard will open the backup volume.

d. Navigate the volume to select the files and folders you would like to restore. Then click **Next**.

e. Select a restore location for the file. The default file path will work if you are restoring the file to its original location. Click **Next**.

f. The wizard will restore the file. If a copy of the file already exists in the location you've chosen, Windows will ask you if you would like to replace the file in the destination folder with the one from the backup. Select **Copy and Replace** and your file will be successfully restored. Click the **Close** button to close the wizard.

### 4.4 Restore Files From Mac Client Computers

a. Open **Time Machine** in the dock or in the Applications folder. The Time Machine window will open.

b. Use the timeline on the right side of the screen to navigate back to the point in time you wish to restore from.

c. Navigate to the files or folders you wish to restore. Highlight them and click the **Restore** button in the bottom right corner.

## 5 Restore a DataHarbor Server

There are three methods for restoring a DataHarbor server. Choose the method appropriate to your situation.

### 5.1 Restore From a Failed Primary Hard Drive

*Use these instructions if:*

- *The primary hard drive in your DataHarbor has failed.*
- **And** *you have a brand new replacement drive that is the same capacity or larger as the failed drive.*

**NOTE:** Do **not** replace your failed primary hard drive with one of your encrypted backup drives. You **must** use a non-encrypted drive as your primary hard drive and follow these instructions since the DataHarbor will only access encrypted data through its removable drive bay.

a. Power down the DataHarbor and unplug all cables from the back of the unit. Then remove it from the rack or storage area.

b. Open the top of the DataHarbor case by removing the two thumb screws and the safety screw securing the cover. Set the cover aside.

c. Unplug and remove the hard drive from the case. To remove the drive, untwist the thumb screw securing the hard drive bracket in place. Then slide the drive away from the thumb screw and lift it out of the bracket.

d. Mount the new replacement drive into the DataHarbor. Line up the new drive's screw holes with the mounting pins on the side of the bracket opposite the thumb screw and slide it into the bracket. Then twist the thumb screw to secure the mounting bracket. Plug the SATA data cable into the drive, but do **not** plug the power cable into the drive yet.

e. If the latest backup drive is not already inserted into the removable bay, insert it now and secure it by turning the DataPort latch 90 degrees clockwise. This will be the drive the DataHarbor will boot from and use to mirror to the replacement primary hard drive.

f. Connect the monitor, keyboard, mouse, and power cables back into the rear of the unit.

g. Power on the DataHarbor. The RAID alarm will begin beeping. Press the **Enter** button to mute the alarm.

h. After the DataHarbor boots up, plug in the SATA power cable into the replacement primary hard drive.

i. Once the drive spins up, the LCD screen will ask you if you would like to add a new drive. Press the **Enter** button. The RAID will now automatically begin rebuilding* from the DataPort 10 to the primary drive.

j. Once the rebuilding process is finished, restart the server so that it will boot from the primary drive.

You have successfully replaced the primary drive and restored your server. Replace the cover using the two thumb screws and remount it into your rack setup or place it back into its storage area.

*The rebuild process will take several hours to complete, during which you can still use the DataHarbor. Simply reconnect the Ethernet network cable to the rear of the unit.

### 5.2 Rebuild a Degraded RAID

*Use these instructions if:*

- *Power to the DataPort 10 bay has been shut off or the drive inside the carrier has failed.*
- **And** *the DataHarbor's LCD screen reports that the mirror is degraded.*

a. Mute the RAID alarm by pressing the **Enter** button.

b. Remove the drive carrier from the DataHarbor and replace the drive inside the carrier with a known good hard drive.

c. Reinsert the drive carrier into the DataHarbor and turn the latch 90 degrees clockwise to power the new drive.

d. Wait a few seconds and the LCD will ask if you would like to add a new drive. Press the **Enter** button to confirm. The RAID will now automatically begin rebuilding. This process will take several hours.

### 5.3 Restore to a New DataHarbor with Identical Hardware

*Use these instructions if:*

- *You are replacing your old DataHarbor with a brand new DataHarbor that has identical internal hardware.*
- **And** *you have retained the primary hard drive from your old DataHarbor and are not restoring from an encrypted backup drive.*

a. Power down the DataHarbor and unplug all cables from the back of the unit. Then remove it from the rack or storage area.

b. Open the top of the new DataHarbor case by removing the two thumb screws and the Phillips-head screw securing the cover. Set the cover aside.

c. Unplug and remove the hard drive from the case. To remove the drive, untwist the thumb screw securing the hard drive bracket in place. Then slide the drive away from the thumb screw and lift it out of the bracket.

d. Mount the primary drive from your old DataHarbor into the new DataHarbor. Line up the new drive's screw holes with the mounting pins on the side of the bracket opposite the thumb screw and slide it into the bracket. Then twist the thumb screw to secure the mounting bracket. Plug the SATA data and power cables into the drive.

e. Put the cover back on the case and screw it back down.

f. Mount the new DataHarbor into your rack or place it back into your storage area. Connect the appropriate cables into the rear of the unit.

g. Remove the carrier from the DataHarbor. If there is no drive installed into the carrier, install one.

h. Power on the DataHarbor. The RAID alarm will begin beeping. Press the **Enter** button to mute the alarm.

i. Replace the carrier into the DataHarbor and lock it into place. Wait a few seconds as the drive spins up and the LCD will then ask if you would like to add a new drive. Press the **Enter** button to select 'Yes'. The RAID will now automatically begin rebuilding, populating the data from the primary drive inside the DataHarbor to the secondary drive that came inside the carrier.

You have successfully restored your server.

### 5.4 Restore to a New DataHarbor From an Encrypted Backup Drive

*Use these instructions if:*

- *You are replacing your old DataHarbor server with a DataHarbor that is newer or different from your original configuration from an encrypted backup drive.*
- **Or** *you are restoring your DataHarbor from an encrypted backup drive.*

a. Plug a keyboard, mouse, and monitor into the new DataHarbor and power on the unit.

b. After the DataHarbor starts up, follow the setup procedure laid out in Section 2.2.

c. Install your backup drive into a DataPort SecureDock (sold separately) and attach the SecureDock to the DataHarbor via eSATA or USB (eSATA is recommended for faster transfer times).

d. Insert your backup Security Key from your original DataHarbor configuration into the SecureDock's Security Key port.

e. Turn the SecureDock on. Windows Storage Server should detect the disk after a few seconds and mount the drive.

f. Open **Server Manager** from the Task Bar. In the navigation pane to the left, expand the **Storage** section and select **Windows Server Backup**.

g. On the Actions pane to the right, select **Recover…** to open the Recovery Wizard.

h. The wizard will ask where the backup is stored. Select **A Backup stored in another location** and click **Next**.

i. The wizard will then ask you to choose the location type. Select **Local Drive** and click **Next**.

j. The next screen should already have the SecureDock drive selected, so click **Next** again.

k. Choose the server to recover. Select your original server name from the list and click **Next**.

l. Select the most recent backup from the calendar and select **Next**.

m. Select **System State** as the recovery type and click **Next**.

n. Select **Recover to an Alternate Location** and select the **Browse** button. Choose the local C: drive from the file listing and click **OK**. Then click **Next**.

o. Click the **Recover** button to begin the recovery process. This will take approximately 15-20 minutes to complete.

p. When the recovery is complete, you must move the client backups to the new DataHarbor. Click on the **Start** menu and select **Computer**. Navigate to the following folder on the SecureDock drive: <SecureDock>:/Server Folders/

q. Copy the **Client Computer Backups** folder and paste it into C:/Server Folders/. If Windows asks you to overwrite any files or folders, select **Yes**. This process will take several hours, depending on the size of your backups.

r. When the file copy is finished, remove the SecureDock from the DataHarbor and restart the server.

You have successfully restored your server.

### 5.5 Migrate Data to a Newer Version of DataHarbor

*Use these instructions if:*

- *You are replacing your old DataHarbor server with a DataHarbor that is newer or different from your original configuration.*
- **And** *you have retained the primary hard drive from your old DataHarbor and are not restoring from an encrypted backup drive.*

a. Power down your original DataHarbor and unplug all cables from the back of the unit. Then remove it from the rack or storage area.

b. Open the top of your original DataHarbor case by removing the two thumb screws and the Phillips-head screw securing the cover. Set the cover aside.

c. Unplug and remove the hard drive from the case. To remove the drive, untwist the thumb screw securing the hard drive bracket in place. Then slide the drive away from the thumb screw and lift it out of the bracket.

d. Insert the drive into an external enclosure and attach that enclosure to your brand new DataHarbor.

e. Turn both the enclosure and the DataHarbor on. After logging into Windows Storage Server loads, it should detect the disk and mount the drive.

f. Open **Server Manager** from the Task Bar. In the navigation pane to the left, expand the **Storage** section and select **Windows Server Backup**.

g. On the Actions pane to the right, select **Recover…** to open the Recovery Wizard.

h. The wizard will ask where the backup is stored. Select **A Backup stored in another location** and click **Next**.

i. The wizard will then ask you to choose the location type. Select **Local Drive** and click **Next**.

j. The next screen should already have the external drive selected, so click **Next** again.

k. Choose the server to recover. Select your original server name from the list and click **Next**.

l. Select the most recent backup from the calendar and select **Next**.

m. Select **System State** as the recovery type and click **Next**.

n. Select **Recover to an Alternate Location** and select the **Browse** button. Choose the local C: drive from the file listing and click **OK**. Then click **Next**.

o. Click the **Recover** button to begin the recovery process. This will take approximately 15-20 minutes to complete.

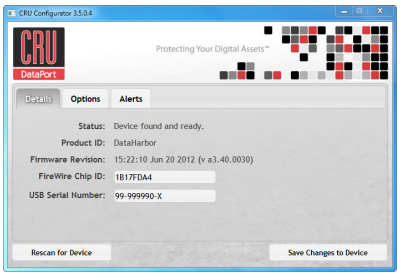
p. When the recovery is complete, you must move the client backups to the new DataHarbor. Click on the **Start** menu and select **Computer**. Navigate to the following folder on the external drive: <External Drive>:/Server Folders/

q. Copy the **Client Computer Backups** folder and paste it into C:/Server Folders/. If Windows asks you to overwrite any files or folders, select **Yes**. This process will take several hours, depending on the size of your backups.

r. When the file copy is finished, remove the enclosure from the DataHarbor and restart the server.

You have successfully migrated your files to your new DataHarbor server.

## 6 Buzzer and Temperature Configuration




The DataHarbor is compatible with CRU Configurator 3.5 or higher, which allows IT administrators to change internal settings to meet individual needs. Configurator allows the user to set the password, enable and disable audible alarms, and change temperature alarms and warnings settings. To download Configurator and the full Configurator manual, visit www.wiebetech.com/software/configurator.php.

### 6.1 Accessing DataHarbor's Settings

a. Power down the DataHarbor and unplug all cables from the back of the unit. Then remove it from the rack or storage area.

b. Open the top of the new DataHarbor case by removing the two thumb screws and the Phillips-head screw securing the cover. Set the cover aside.

c. Disconnect the 3 SATA data cables from the PCA board mounted directly behind the LCD Display.

d. Connect a USBA-to-USB-mini-B cable to the mini USB connector located on the PCA board and connect the other side of the cable to a computer.

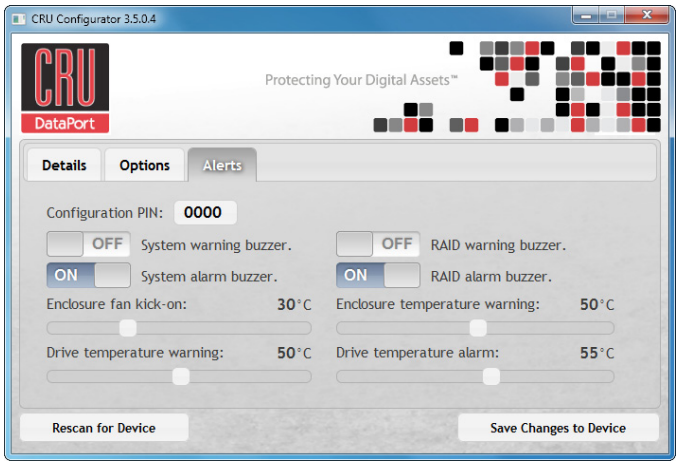
e. Download and install Configurator onto the computer and then open it.

f. Customize the settings to your desired preferences.

g. Click **Save Changes to Device**.

Be sure to reconnect the SATA data cables to their correct positions on the PCA board before using the DataHarbor

### 6.2 Customizable Options




The following options are available on the **Alerts tab** of the Configurator:

**Configuration PIN**
This feature allows you to set a PIN to prevent unauthorized configuration. The default PIN is 0000. The DataHarbor only requires you to enter a PIN if a different value has been set.

**Buzzers**
Place a check in the boxes to indicate which warning/alarm buzzers you want to be activated or remove a check from the boxes next to the buzzers you want to deactivate.

**System Warning Buzzer**
This buzzer will sound when a drive reaches the temperature set using the **Drive temperature warning** slider below. This buzzer is disabled by default. As a visual alert, the System Status LED will glow amber when the temperature is reached, regardless of whether the buzzer is enabled or not.

**System Alarm Buzzer**
This buzzer will sound on 3 occasions:

- When a drive reaches the temperature set using the **Drive temperature alarm** slider below
- When the enclosure reaches the temperature set using the **Enclosure temperature warning** slider below
- When the fan fails

As a visual alert, the System Status LED on your DataHarbor will glow red when any of these three situations occur, regardless of whether the buzzer is enabled or not.

**RAID Warning Buzzer**
This buzzer will sound when the DataHarbor is in degraded RAID mode (a drive has failed and is in need of rebuild or the RAID is rebuilding). This buzzer is disabled by default. The Mirror Status LED will glow amber if this occurs, regardless of whether the buzzer is enabled or not.

**RAID Alarm Buzzer**
This buzzer will sound when the RAID has failed or is invalid. The Mirror Status LED will glow red if this occurs, regardless of whether the buzzer is enabled or not.

**Temperature Sliders**
When your DataHarbor reaches a certain temperature, buzzers will sound if they are enabled (see the "Buzzers" subsection above) and the fan will kick on. You may want to change these default temperatures according to your environment. With these sliders, you can change the default temperatures of the:

- Enclosure fan kick-on
- Enclosure temperature warning
- Drive temperature warning
- Drive temperature alarm

## 7 Best Practices for a Proper Backup Strategy

Since there are many things besides hard drive failure that can compromise your data (e.g. malware, theft, fire, etc.), CRU-DataPort suggests the following steps to ensure your data remains intact:

- Ensure you have at least three different copies of your data. The DataHarbor allows you to do this by maintaining a daily backup of your original copy and mirroring it to a removable hard drive.
- Retain a weekly backup offsite. Remove the external hard drive and take it offsite with you on a weekly basis. Insert a third hard drive into the DataHarbor and let it rebuild the data over the weekend so that the DataHarbor's mirror is retained.

Any single copy of your important data must always be considered at risk. Without an effective backup strategy, recovering data may be impossible, or the cost of data recovery may be quite expensive. The CRU warranty does not cover costs associated with data loss (nor do the warranties of other storage manufacturers).

Plan accordingly and backup data to minimize downtime!

## 8 Encryption

- The DataHarbor uses full disk hardware encryption to encrypt the entire contents of the drive—including the boot sector, operating system and all files—without performance degradation.
- A Security Key must be installed prior to powering on an enclosure for the data to be decrypted on the drive. The DataHarbor has a Security Key internally connected at all times, but also includes two additional external Security Keys. Always store these keys offsite away from your backups so that in the event that the DataHarbor suffers catastrophic damage or is stolen, your backup data is still retrievable.
- The same or a duplicate key must be used in order to access the data. **There is no "back door" to access the data; lost keys make data recovery virtually impossible.**

## 9 Technical Specifications

| | |
|---|---|
| Product Name | DataHarbor |
| Interface Types & Speeds | • Gigabit Ethernet: up to 1 Gbps<br>• eSATA: up to 3 Gbps<br>• USB 3.0: up to 5 Gbps<br>• USB 2.0: up to 480 Mbps<br>• Serial RS-232: up to 11520 bit/s |
| Drive Types Supported | 3.5" SATA* Hard Drives<br>*SATA III Drives must be jumpered to run at 3.0 Gbps transfer speed |
| Connectors | Two (2) Gigabit Ethernet connectors<br>Two (2) eSATA connectors<br>Two (2) USB 3.0 connectors<br>Four (4) USB 2.0 connectors (3 rear, 1 front)<br>One (1) Serial connector<br>One (1) PS/2 connector<br>One (1) VGA connector<br>One (1) Speaker connector<br>One (1) Line In connector<br>One (1) Microphone connector |
| Server Operating System | Windows Storage Server 2008 R2 Essentials |
| Client Operating System Requirements | • Windows XP SP3 32-bit, Vista SP2, 7, or 8<br>• Mac OS 10.5 Leopard or Mac OS 10.6 Snow Leopard*<br>*Client Backups must be manually configured |
| Compliance | EMI Standard: FCC Part 15 Class B, CE<br>EMC Standard: EN55022, EN55024 |
| Shipping Weight | 24 pounds (includes accessories) |
| Product Dimensions | 16.14" x 1.72" x 14.17" (410mm x 44mm x 360mm) |
| Technical Support | Please contact your IT administrator if you have questions about Microsoft Windows Storage Server 2008 R2 Essentials, or visit http://technet.microsoft.com/en-us/library/ff953176.aspx<br><br>Contact us at www.cru-dataport.com/support for support related to your DataHarbor hardware. We also offer phone support at (800) 260-9800 or (360)-816-1800. |

DataHarbor is a trademark of CRU Acquisitions Group, LLC. Other marks are the property of their respective owners. © 2010 CRU Acquisitions Group, LLC. All rights reserved.

**Product Warranty**
CRU-DataPort (CRU) warrants this product to be free of significant defects in material and workmanship for a period of two years from the original date of purchase. CRU's warranty is nontransferable and is limited to the original purchaser.

**Limitation of Liability**
The warranties set forth in this agreement replace all other warranties. CRU expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CRU dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CRU or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CRU product or service, even if CRU has been advised of the possibility of such damages. In no case shall CRU's liability exceed the actual money paid for the products at issue. CRU reserves the right to make modifications and additions to this product without notice or taking on additional liability.

**FCC Compliance Statement:** "This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a home or commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:
1) Ensure that the case of your attached drive is grounded.
2) Use a data cable with RFI reducing ferrites on each end.
3) Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
4) Reorient or relocate the receiving antenna.